

Số: /QĐ-ĐPTTH

Ninh Thuận, ngày tháng 5 năm 2021

## **QUYẾT ĐỊNH**

### **Quy chế Bảo vệ bí mật Nhà nước, bảo đảm an toàn, an ninh thông tin tại Đài Phát thanh và Truyền hình tỉnh Ninh Thuận**

#### **GIÁM ĐỐC ĐÀI PHÁT THANH VÀ TRUYỀN HÌNH TỈNH NINH THUẬN**

*Căn cứ Quyết định số 03/2021/QĐ-UBND ngày 24/02/2021 của Chủ tịch Ủy ban nhân dân tỉnh Ninh Thuận về việc Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Đài Phát thanh và Truyền hình tỉnh Ninh Thuận;*

*Căn cứ Luật Công nghệ thông tin và các văn bản hướng dẫn thi hành;*

*Căn cứ Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành;*

*Căn cứ Pháp lệnh Bảo vệ bí mật Nhà nước và các văn bản hướng dẫn;*

*Căn cứ Kế hoạch số 1757/KH-UBND ngày 26/4/2019 của UBND tỉnh Ninh Thuận triển khai thi hành Luật Bảo vệ bí mật nhà nước;*

*Căn cứ Văn bản số 181/UBND-TCDNC ngày 06/5/2021 của UBND tỉnh Ninh Thuận về chấp hành quy định của pháp luật khi tham gia dịch vụ bưu chính phục vụ các cơ quan Đảng, Nhà nước;*

*Theo đề nghị của Trưởng phòng Tổ chức và Hành chính.*

## **QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này bổ sung Quy chế Bảo vệ bí mật Nhà nước, bảo đảm an toàn, an ninh thông tin tại Đài Phát thanh và Truyền hình tỉnh Ninh Thuận.

**Điều 2.** Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 481/QĐ-ĐPTTH ngày 29/5/2019 của Đài Phát thanh và Truyền hình tỉnh Ninh Thuận về Quy chế Bảo vệ bí mật Nhà nước, bảo đảm an toàn, an ninh thông tin.

Trưởng phòng Tổ chức và Hành chính, các phòng chuyên môn và viên chức có liên quan chịu trách nhiệm thi hành Quyết định này./.

#### **Nơi nhận:**

- Như Điều 2;
- PA03, Công an tỉnh;
- Ban Giám đốc;
- CBVC;
- Lưu VT.

**GIÁM ĐỐC**

**Nguyễn Minh Hà**

## **BỔ SUNG QUY CHẾ**

### **Bảo vệ bí mật Nhà nước, bảo đảm an toàn, an ninh thông tin tại Đài Phát thanh và Truyền hình tỉnh Ninh Thuận**

*(Ban hành kèm theo Quyết định số /QĐ-ĐPTTH ngày tháng 5 năm 2021  
của Đài Phát thanh và Truyền hình tỉnh Ninh Thuận)*

## **Chương I NHỮNG QUY ĐỊNH CHUNG**

### **Điều 1. Phạm vi và đối tượng áp dụng:**

1. Quy chế này quy định việc quản lý và sử dụng bí mật Nhà nước (BMNN) thuộc phạm vi quản lý của Đài Phát thanh và Truyền hình tỉnh Ninh Thuận
2. Quy chế này được áp dụng đối với cán bộ, viên chức liên quan đến việc khai thác, sử dụng bí mật Nhà nước thuộc phạm vi Đài Phát thanh và Truyền hình tỉnh Ninh Thuận quản lý.

### **Điều 2. Bí mật Nhà nước thuộc Đài Phát thanh và Truyền hình tỉnh Ninh Thuận quản lý và bảo vệ gồm:**

1. Các văn bản, tài liệu có độ mật (gọi chung là tài liệu mật) của các cơ quan ở Trung ương và địa phương gửi đến Đài Phát thanh và Truyền hình tỉnh Ninh Thuận.
2. Tài liệu quy hoạch cán bộ và hồ sơ nhân sự cán bộ, viên chức của Đài.
3. Hồ sơ, tài liệu đang thanh tra, kiểm tra, báo cáo kết quả thanh tra chưa công bố.
4. Số liệu thống kê, kế toán, thu chi của Đài chưa được phép công bố.
5. Số liệu, tài liệu đấu thầu, xét thầu các dự án của Đài đang trong quá trình xem xét chưa công bố.
6. Các báo cáo, văn bản khác có sử dụng tin, tài liệu thuộc danh mục bí mật nhà nước độ mật của các cơ quan khác.
7. Đề tài nghiên cứu khoa học trong giai đoạn nghiên cứu, làm thí nghiệm chưa được công bố.

### **Điều 3. Những hành vi nghiêm cấm**

1. Nghiêm cấm mọi hành vi thu thập, làm lộ, làm mất, chiếm đoạt, mua bán tiêu huỷ trái phép tài liệu mật của Đài.
2. Nghiêm cấm các tổ chức và cá nhân cung cấp cho cơ quan báo chí, xuất bản hoặc các cơ quan đại chúng khác các tài liệu mật của Đài Phát thanh và Truyền hình tỉnh Ninh Thuận khi không được phép của người có thẩm quyền.
3. Nghiêm cấm các tổ chức và cá nhân tự nghiên cứu, sản xuất, sử dụng mật mã để tiến hành các hoạt động xâm phạm an ninh quốc gia và các hành vi

khác vi phạm quy định về công tác giữ gìn, bảo vệ bí mật nhà nước của Đài Phát thanh và Truyền hình tỉnh Ninh Thuận.

4. Nghiêm cấm các tổ chức và cá nhân vận chuyển tài liệu, vật mang bí mật nhà nước qua dịch vụ bưu chính phục vụ các cơ quan Đảng, Nhà nước (dịch vụ KT1).

#### **Điều 4. Đảm bảo an toàn, an ninh thông tin**

1. Thường xuyên phổ biến, quán triệt và cập nhật những quy định về an toàn thông tin và hướng dẫn cán bộ, viên chức thực hiện đúng hướng dẫn về an toàn, an ninh thông tin nhằm nâng cao nhận thức và trách nhiệm về an toàn thông tin.

2. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thu hồi chức năng này khi đã sử dụng xong. Đối với các đơn vị có mạng máy tính thuộc mạng cục bộ (LAN) thì tuyệt đối không được tự ý kết nối thêm các máy vi tính, thiết bị ngoại vi (máy tính xách tay, thiết bị lưu trữ di động, bộ phát sóng wifi...) vào hệ thống mạng của cơ quan khi chưa đảm bảo điều kiện an ninh. Không được sử dụng các loại thiết bị lưu trữ ngoài để sao chép, lưu trữ các tài liệu quan trọng, đặc biệt là các thiết bị lạ, chưa được kiểm soát.

3. Các máy vi tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy để tránh bị các tin tặc lợi dụng tấn công vào hệ thống thông tin của máy vi tính.

4. Các máy tính kết nối mạng phải thường xuyên quét vi rút. Khi nhận thư điện tử phải kiểm tra nguồn gốc gửi rõ ràng, các tập tin đính kèm phù hợp với nội dung thư và người gửi thư trước khi mở hay tải tập tin về máy tính. Tuyệt đối không được mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng, các đường liên kết (link) lạ, không rõ nguồn gốc để tránh vi rút, phần mềm gián điệp lây nhiễm máy vi tính.

6. Khai thác tài nguyên Internet có chọn lọc, không vào các trang web lạ, không bấm vào các đường liên kết, biểu tượng quảng cáo không rõ nội dung và không cài đặt phần mềm không rõ nguồn gốc.

7. Phải đặt mật khẩu cho máy vi tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình), Sử dụng các thiết bị lưu trữ thông tin (USB, Thẻ nhớ...) đảm bảo an toàn, đúng cách để phòng ngừa vi rút, phần mềm gián điệp xâm nhập máy vi tính phá hoại, đánh cắp thông tin.

#### **Điều 5. Nguyên tắc bảo đảm an toàn thông tin mạng và ứng dụng công nghệ thông tin**

1. Các phòng, cán bộ và viên chức có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của các phòng, cán bộ và viên chức phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của Đài, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của Đài.

3. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

4. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

## **Điều 6. Các hành vi bị nghiêm cấm**

1. Thu thập, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy, trao đổi, cung cấp trái phép tài liệu mật và lạm dụng việc bảo vệ BMNN để che dấu hành vi vi phạm pháp luật, xâm phạm quyền, lợi ích hợp pháp của các cơ quan, tổ chức và công dân hoặc làm cản trở việc thực hiện các kế hoạch Nhà nước được quy định tại Điều 3 Pháp lệnh bảo vệ BMNN.

2. Sử dụng máy tính nối mạng Internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung BMNN; cài cắm các thiết bị lưu trữ tài liệu có nội dung BMNN vào máy vi tính nối mạng Internet; trao đổi thông tin BMNN qua điện thoại; sử dụng điện thoại di động, micro vô tuyến, thiết bị có tính năng ghi âm, thu phát tín hiệu trong các cuộc họp có nội dung BMNN dưới mọi hình thức; cung cấp thông tin, tài liệu và đưa thông tin BMNN trên báo chí, ấn phẩm xuất bản, các trang thông tin điện tử (Website), được quy định tại khoản 2, điều 5 Quyết định số 71/2004/QĐ-BCA ngày 29/01/2004 của Bộ trưởng Bộ Công an về đảm bảo an toàn, an ninh trong hoạt động quản lý, cung cấp sử dụng dịch vụ Internet tại Việt Nam và các văn bản quy phạm pháp luật có liên quan khác.

3. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

4. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

5. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

6. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

7. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

8. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự,

thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

### **Điều 7. Quản lý người dùng đảm bảo an toàn, an ninh thông tin**

1. Quản lý chặt chẽ tài khoản của các hệ thống thông tin. Đối với các phần mềm nghiệp vụ của Đài đã cung cấp tài khoản cho cán bộ và viên chức để thực hiện nhiệm vụ thì khi cán bộ và viên chức đã nghỉ việc, chuyển công tác phải hủy tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin.

2. Yêu cầu cán bộ và viên chức khi đặt mật khẩu đăng nhập vào các hệ thống thông tin phải phải đặt mật khẩu với độ an toàn cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, \$, %,...) và phải được thay đổi ít nhất 6 tháng/lần.

3. Cán bộ và viên chức chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

## **Chương II**

### **TRÁCH NHIỆM CỦA CÁC PHÒNG, CÁN BỘ-VIÊN CHỨC CÓ LIÊN QUAN TRONG VIỆC BẢO VỆ BÍ MẬT NHÀ NƯỚC**

#### **Điều 8. Trách nhiệm của Trưởng các phòng và viên chức có liên quan**

- Chịu trách nhiệm trực tiếp trước Giám đốc Đài về công tác bảo vệ BMNN thuộc của phòng do mình phụ trách.

- Trên cơ sở lĩnh vực công tác được giao tham mưu cho Giám đốc Đài:

+ Xác định độ mật và phạm vi lưu hành của tài liệu, vật mang BMNN thuộc phạm vi Đài quản lý;

+ Quyết định việc hủy tài liệu, vật mang BMNN;

+ Quy định chuyển loại tài liệu có độ mật sang tài liệu không có độ mật khi tài liệu, vật mang BMNN đã hết giá trị BMNN (tài liệu có độ mật sau khi đã công bố);

+ Duyệt phổ biến, nghiên cứu tin thuộc phạm vi BMNN theo đúng đối tượng, phạm vi cần được phổ biến hoặc nghiên cứu; duyệt ghi chép, ghi âm, ghi hình tài liệu, vật mang BMNN (bảo vệ như tài liệu gốc);

+ Đảm bảo cơ sở vật chất; tổ chức công tác soạn thảo, in sao, chụp, phát hành, phổ biến, lưu trữ, quản lý, khai thác, vận chuyển tin, tài liệu, vật mang BMNN theo quy định của Pháp lệnh Bảo vệ bí mật nhà nước; Nghị định số 33/2002/NĐ-CP ngày 28/3/2002 của Chính phủ và các quy định khác của bộ, ngành có thẩm quyền;

+ Đăng ký các phát minh, sáng chế, giải pháp hữu ích có nội dung thuộc phạm vi bí mật nhà nước tại Sở Khoa học và Công nghệ tỉnh Ninh Thuận (nếu có).

#### **Điều 9. Trách nhiệm của lãnh đạo phòng Tổ chức và Hành chính**

- Thực hiện các nhiệm vụ quy định tại Điều 5 của Quy chế này thuộc nhiệm vụ của Văn phòng.

- Hướng dẫn, đôn đốc, kiểm tra, theo dõi việc thực hiện của các phòng; tham mưu đề xuất Giám đốc các biện pháp bảo đảm an toàn BMNN từ việc bố trí, bảo dưỡng, thay thế, sử dụng các thiết bị, phương tiện điện tử, công nghệ thông tin tại cơ quan.

- Báo cáo định kỳ và đột xuất về công tác Bảo vệ BMNN; tổ chức công tác sơ kết, tổng kết theo quy định.

**Điều 10.** Trách nhiệm của viên chức và các cá nhân có liên quan đến BMNN (gọi chung là người có liên quan đến BMNN) bao gồm: Người trực tiếp soạn thảo, chỉnh lý tài liệu liên quan đến BMNN; người làm công tác giao liên văn thư; bảo quản, lưu giữ, xử lý tài liệu, vật mang BMNN, người làm công tác liên quan đến BMNN phải:

1. Cam kết bảo vệ BMNN.

2. Thực hiện nghiêm túc các quy định tại Nghị định số 33/2002/NĐ-CP ngày 28 tháng 3 năm 2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh Bảo vệ BMNN và Thông tư số 12/2002/TT-BCA(A11) ngày 13 tháng 9 năm 2002 của Bộ Công an hướng dẫn thực hiện Nghị định số 33/2002/NĐ-CP ngày 28 tháng 3 năm 2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh Bảo vệ bí mật nhà nước.

- Người soạn thảo có nội dung BMNN phải căn cứ danh mục BMNN để đề xuất mức độ mật từng loại tài liệu, vật mang BMNN.

- Việc sao chụp tài liệu, vật mang BMNN phải tiến hành ở nơi đảm bảo bí mật, an toàn; chỉ in, sao chụp đúng số bản đã được quy định, hủy ngay các bản dư thừa, hư hỏng; đóng các loại dấu bảo mật lên các tài liệu, vật mang BMNN sau khi được duyệt.

- Chỉ được phổ biến, nghiên cứu tin thuộc phạm vi BMNN theo đúng thẩm quyền, đối tượng, phạm vi cần được phổ biến hoặc nghiên cứu đã được cấp thẩm quyền phê duyệt.

- Khi vận chuyển, giao nhận những tài liệu, vật mang BMNN ở trong nước phải có đủ phương tiện bảo quản và lực lượng bảo vệ và phải do cán bộ làm công tác bảo mật hoặc cán bộ được phân công thực hiện. Trường hợp vận chuyển, giao nhận theo đường bưu điện thì thực hiện theo quy định riêng của Ngành Bưu điện. Không tự ý bóc mở bì thư có ghi tên, chức vụ của người nhận. Việc chuyển phát bằng phương tiện viễn thông và máy tính phải được mã hóa theo quy định của Pháp luật về cơ yếu. Việc mang tài liệu đi công tác trong nước, ra nước ngoài phải do người có thẩm quyền theo quy định của pháp luật đồng ý bằng văn bản.

- Việc cung cấp thông tin thuộc phạm vi BMNN cho cơ quan, tổ chức, công dân Việt Nam và các tổ chức, cá nhân nước ngoài phải được sự đồng ý của cấp có thẩm quyền (cung cấp thông tin BMNN cho tổ chức, công dân Việt Nam tài liệu vật mang BMNN thuộc độ Tuyệt mật, Tối mật do Chủ tịch UBND tỉnh

duyet; thuộc độ Mật do Giám đốc Đài duyet. Đối với tổ chức, cá nhân nước ngoài: Bí mật thuộc độ Tuyệt mật, Tối mật do Bộ trưởng Bộ Công an duyet (riêng lĩnh vực Quốc phòng do Bộ trưởng Bộ Quốc phòng duyet); bí mật thuộc độ Mật do Chủ tịch UBND tỉnh duyet. Cơ quan tổ chức và cá nhân không được cung cấp tin thuộc phạm vi BMNN cho cơ quan báo chí.

- Việc tiêu hủy tài liệu, vật mang BMNN do Giám đốc Đài quyết định theo quy định của pháp luật và phải đảm bảo yêu cầu không để lộ lọt, phải làm thay đổi hình dạng và tính năng tác dụng không thể phục hồi được.

**Điều 11.** Trang Thông tin điện tử của Đài phải chấp hành nghiêm các quy định về bảo vệ BMNN theo Luật Báo chí, các văn bản pháp luật về bảo vệ bí mật nhà nước và Quy chế này.

### **Chương III**

#### **TRÁCH NHIỆM CỦA CÁC PHÒNG, CÁN BỘ, VIÊN CHỨC CÓ LIÊN QUAN TRONG VIỆC ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN**

#### **Điều 12. Trách nhiệm của Trưởng các phòng, Tổ chức giúp việc**

1. Tổ chức tuyên truyền, phổ biến quán triệt cho viên chức các văn bản chỉ đạo của Trung ương, của Tỉnh ủy, UBND tỉnh và các quy định của pháp luật về đảm bảo an toàn, an ninh thông tin nhằm nâng cao nhận thức cho viên chức về nguy cơ mất an toàn, an ninh hệ thống thông tin và có biện pháp để phòng ngừa, ngăn chặn khi có sự cố xảy ra.

2. Tổ chức thực hiện các quy định tại Quy chế này và các quy định pháp luật có liên quan; chịu trách nhiệm trước Lãnh đạo Đài trong công tác đảm bảo an toàn, an ninh thông tin của cơ quan.

3. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải chỉ đạo xử lý khắc phục kịp thời và thông báo cho lãnh đạo phòng Tổ chức và Hành chính biết. Trường hợp không khắc phục được thì báo phòng Tổ chức và Hành chính để báo Tổ ứng cứu sự cố máy tính trên địa bàn tỉnh để hướng dẫn, hỗ trợ khắc phục.

4. Phối hợp chặt chẽ trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

5. Định kỳ hoặc đột xuất, báo cáo phòng Tổ chức và Hành chính về tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại phòng mình.

#### **Điều 13. Trách nhiệm của viên chức**

1. Trách nhiệm của viên chức được giao phụ trách công nghệ thông tin

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật đảm bảo an toàn an ninh cho hệ thống thông tin của cơ quan, đơn vị.

b) Thông báo cho cơ quan biết và có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất an toàn, an ninh thông tin do vi rút, phần mềm gián điệp... gây ra.

c) Phối hợp với các phòng và viên chức thuộc Đài có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn, an ninh thông tin.

## 2. Trách nhiệm của viên chức

a) Chấp hành nghiêm túc các quy định về an toàn, an ninh thông tin được quy định tại Quy chế này cũng như quy định khác của pháp luật có liên quan, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin.

b) Khi phát hiện sự cố phải báo ngay với lãnh đạo đơn vị và bộ phận chuyên trách CNTT để kịp thời ngăn chặn, xử lý.

## **Chương IV TỔ CHỨC THỰC HIỆN**

### **Điều 14. Khen thưởng, xử lý vi phạm**

1. Cán bộ, viên chức có thành tích xuất sắc trong công tác bảo vệ BMNN, bảo đảm an toàn, an ninh thông tin của Đài được khen thưởng theo quy định của pháp luật.

2. Cán bộ, viên chức vi phạm các quy định của pháp luật về bảo vệ BMNN, an toàn, an ninh thông tin tùy theo tính chất, mức độ vi phạm và hậu quả gây ra sẽ bị xử lý kỷ luật hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

**Điều 15.** Trưởng các phòng chuyên môn thuộc Đài có trách nhiệm triển khai thực hiện nội dung Quy chế này và định kỳ báo cáo công tác bảo vệ BMNN, an toàn, an ninh thông tin theo quy định.

**Điều 16.** Trưởng phòng Tổ chức và Hành chính giúp Giám đốc Đài triển khai thực hiện Quy chế này; phối hợp với các phòng có liên quan thường xuyên rà soát, đề xuất sửa đổi, bổ sung những nội dung không còn phù hợp đảm bảo thực hiện đúng quy định hiện hành về công tác bảo vệ BMNN và an toàn, an ninh thông tin./.

**GIÁM ĐỐC**

**Nguyễn Minh Hà**